TECHNICAL DOCUMENT 2047
August 2014

Personal Area Networks in Tactical Mobile Devices

Brian Visser

SSC Pacific
San Diego, CA 92152-5001

TECHNICAL DOCUMENT 2047
August 2014

Personal Area Networks in Tactical Mobile Devices

Brian Visser

Approved for public release.

SSC Pacific
San Diego, CA 92152-5001

SSC Pacific
San Diego, California 92152-5001

K. J. Rothenhaus, CAPT, USN
Commanding Officer

C. A. Keeney
Executive Director

ADMINISTRATIVE INFORMATION

This work described in this report was performed by the Composeable Services Branch (Code 53628) of the C2 Technology and Experimentation Division (Code 53600), SPAWAR Systems Center Pacific (SSC Pacific), San Diego, CA. The project work is funded by the Science and Technology Initiative (STI) Program at SSC Pacific.

Released by
E. Castro, Head
Composeable Services Branch

Under authority of
C. Raney. Head
C2 Technology and
Experimentation Division

SB

EXECUTIVE SUMMARY

OBJECTIVE

The first objective is to determine if adding personal area networking technologies to current Android apps is easily achievable. The second objective was to determine when each networking technology should be used rather than an alternative method.

METHOD

For the first object, an Android library was written and integrated into an example app. The amount of extra effort and code changes that was required were documented. The second objective method was to send data of pre-determined size and measure the time it takes. The data size was increased over the experiment, and each network type was tested.

CONCLUSION AND SUMMARY

The PAN library was designed to reduce the impact on implementing apps. Therefore, the impact on time and effort is minimal. The app only needs to implement several methods, and manage its own data. Each network type has setup overhead as well as different transmit speeds. For Near Field Communication (NFC), it is recommended to use for data sizes less than 1024 bytes, or to bootstrap another network type. Bluetooth® is recommended for sizes between 1025 bytes and 131072 bytes, and Wi-Fi Direct® for anything larger. These data size recommendations give the best time and power usage.

CONTENTS

Figures

Tables

Code

1. INTRODUCTION

1.1 OPERATIONAL NEED

Marines currently patrolling at the edge of the battlespace possess extremely limited situation awareness (SA). This is mainly due to technological inadequacies. Current SA systems, such as Joint Tactical Common Operation Picture (COP) Workstation (JTCW) or Global Command and Control System (GCCS), were not designed for echelons below the Company level. This is due, in part, to a lack of computer hardware specialized for the tactical environments where these echelons operate. The limitation of size, weight, and power (SWaP) is a major hurdle in designing these systems; laptop computers are ineffective without a consistent power source, which is normally not available to patrols. In addition to the lack of computer resources, robust network infrastructure, both wired and wireless, does not exist. Radio networks, such as PRC-117G, exist in the field, but are not available for non-military frequencies or are used for voice only. Other networks are available but only in limited capacities and are often disconnected, intermittent, and latent (DIL).

Emerging handheld computing technologies offer several solutions to the SWaP and networking issues encountered at the tactical edge. Modern mobile devices have excellent power efficiency and are much smaller and lighter than laptops while maintaining an appropriate level of computational power and usability. Android-powered mobile devices offer a user several new Personal Area Network (PAN) options: Near Field Communication (NFC), Wi-Fi Direct®, and Bluetooth®. These short-range, power-efficient networking technologies help solve networking issues present in tactical environments (see Table 1).

NFC allows a device to read radio-frequency identification (RFID) tags or communicate with another NFC-enabled device using a set of standards: (Standard ECMA-340, 2004; (Standard ECMA-352, 2010; ISO/IEC, 2013). This allows for extremely limited distance, typically less than 4 cm, low-power data transfer. NFC allows for data rates of 106, 212, and 424 Kbit/s (ISO/IEC, 2013).

Wi-Fi Direct® is a standard that allows one device to connect to another directly without traditional infrastructure (Wi-Fi Alliance, 2010). One device runs as a soft-access point and Dynamic Host Configuration Protocol (DHCP) server, while the other device connects as its client. This allows for instant, secure networks with a standard Internet Protocol (IP)-based connection. Wi-Fi Direct inherits many of the benefits and caveats of regular Wi-Fi®. It generally, but not always, uses more power than other technologies, has a longer range, and more throughput. Since Wi-Fi Direct uses standard 802.11 protocols, it can carry data at the highest speeds supported by the devices. The latest approved specification is 802.11n, which has nominal data rates of 54 Mbit/s (more if multiple data streams are used). Draft specifications (ac and ad) have much greater data rates (Wi-Fi Alliance, 2013).

In addition to these relatively new PAN capabilities, an update to the Bluetooth® specification is also available for transferring data (Bluetooth, 2010). Devices with Bluetooth® Specification 4.0 will have two new transmission options: high speed and low energy. These allow for greater data transfer and efficient power utilization, respectively. Bluetooth® high speed has data rates of 24 Mbit/s and Bluetooth® low energy (BLE) has data rates of 200 Kbit/s (Bluetooth, 2010). According to Siekkinen, Hijenkari, and Nurminen. BLE is more efficient than Wi-Fi®. Seikkinen, Hiienkari, Nurminen, and Nieminen (2012) state that "…when the throughput [of Wi-Fi] varies from 16 to 256 KBps, the energy utility ranges from roughly 20 to 240 KB/J which is clearly lower than that of BLE."

Table 1. PAN technologies summary.

Technology	Bandwidth	Distance[1]	Power Consumption
NFC	424 Kbit/s	Nearly touching	Low
Bluetooth® low energy	200 Kbit/s	Short distance	Low
Bluetooth® 4.0 high speed	24,000 Kbit/s	Short distance	Moderate
Wi-Fi Direct®	54,000 Kbit/s	Medium distance	Moderate

1.2 PURPOSE

The Science and Technology Initiative (STI) funds research on personal area networks in tactical mobile devices to determine the usefulness of PAN technologies in commercial off-the-shelf mobile devices for tactical users. Researchers will use several criteria to determine the effectiveness if such networks:

- SWaP – Size Weight and Power is of great concern for all systems used by tactical United States Marine Corps (USMC) personnel. The FY13 MAGTF Roadmap specifically has a section entitled “Lighten the MAGTF” (Deputy Commandant for Combat Development and Integration, 2013). Using less energy in tactical communication will reduce battery usage, which contribute significant weight to the warfighter’s equipment (Erwin, 2011).
- Ease of Use – Ease of use for the end-user is important, as is the amount of training required to field new technology. If warfighters find a new technology easy to use, the more likely it is that they will use it and use it properly.
- Ease of Implementation – Ease of implementation is important from a financial standpoint. An easier to implement technology takes fewer man-hours to integrate into systems, and also introduces less software bugs.

[1] The Bluetooth® specification does not give a distance for operation. Typically, the theoretical distances quoted by some is based on maximum power output based on the three classes of Bluetooth®. For instance, Class 1 Bluetooth® devices are said to transmit 100 m. They transmit at a maximum of 100 mW (20 dBm).

2. PAN EXPERIMENTATION

2.1 PURPOSE

Researchers use PAN experimentation to determine the time it takes to send a certain amount of data. This includes the time for data transmission over the air, as well as the overhead associated with each PAN technology. Researchers use these results to create thresholds for automatic network determination.

2.2 PROCEDURE

Researchers perform the following step-by-step procedure to PAN experimentation.

1. Hold two devices with PAN app open together. The system NFC system will be triggered.
2. Touch and hold the "server" mobile device to send the data.
3. Record data and repeat five times
4. Repeat steps 1 through 3 for each network type, for each message size.

2.3 DATA COLLECTION

This Pan experiment has two data points. The first data point is when the system NFC is initiated. The PAN library's NFC callback method `createNdefMessage(…)` is called. This method includes processing the data from the app as well as data internal to the PAN Library.

The second data point is when the client has completely finished receiving data. If this is only over NFC, it is when the PAN Library is resumed due to a system intent `android.nfc.action.NDEF_DISCOVERED` and ready to process the `PanData`. If Bluetooth of Wi-Fi Direct® is used, the data point is after `mil.navy.pan.data.PanDataClient` has finished receiving data over its socket, and is ready to process the `PanData`.

The process is conducted five times per message size because sending the NDEF message is triggered by user interaction. The results are averaged to obtain a realistic time for a typical user using the system (see Figure 1).

2.4 RESULTS

The full set of raw data can be viewed in the `pan data.xlsx` Excel document. Table 2 provides a PAN data overview.

The thresholds for automatic network determination can be specified from the data set. For maximum user interface (UI) responsiveness, NFC should only be used to transfer small pieces of data. The data should be less than 1024 Bytes. However, for small data sets, NFC has the quickest response with little overhead, making UI responsiveness excellent.

Bluetooth® has an overhead time of approximately 1 sec. Bluetooth® has acceptable transfer times for under 131072 Bytes (0.125 MB) and has excellent reliability. While testing, researchers had no issues setting up or tearing down Bluetooth connections.

Wi-Fi Direct® has the greatest setup time as well as data throughput. This technology should not be used for small amounts of data because of the large overhead setup—approximately 10 sec. For data larger than 131072 Bytes of data, Wi-Fi Direct® is the most practical.

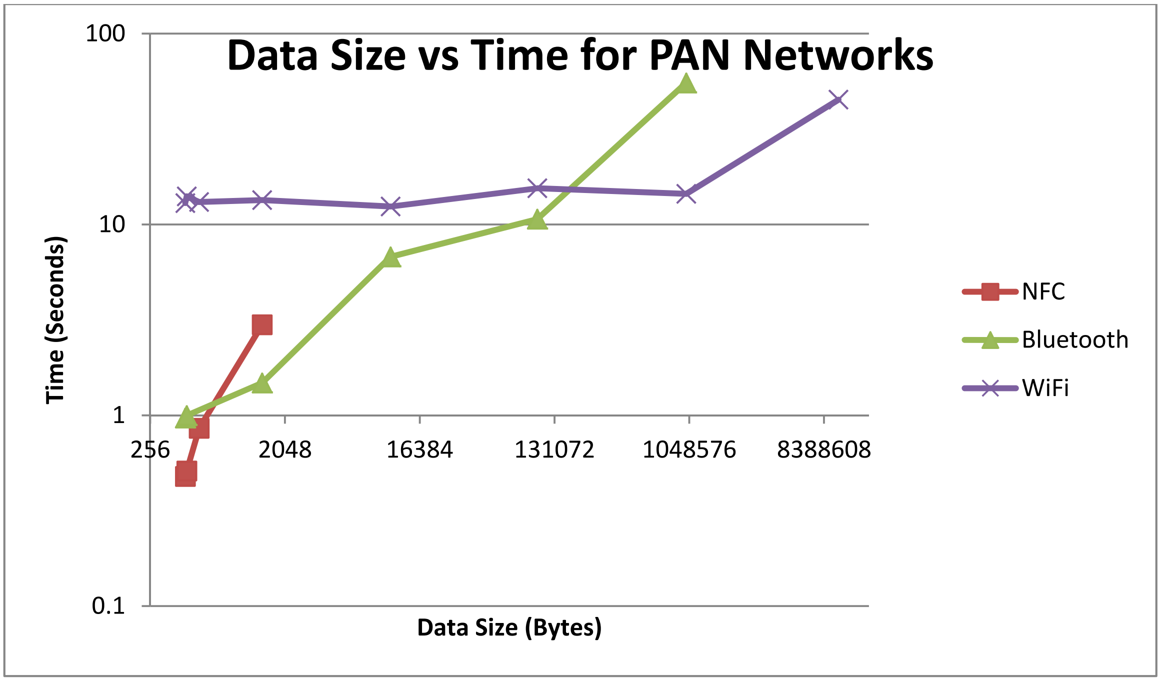

Figure 1. Data size vs. time.

Table 2. PAN data overview.

Technology	Setup Overhead	Recommended Maximum Data Size
NFC	< 0.5 seconds	1024 Bytes
Bluetooth®	~ 1 second	131072 Bytes
Wi-Fi Direct®	~ 10 seconds	

3. EASE OF IMPLEMENTATION

3.1 INTERFACE

For an existing Android app to integrate with the PAN Library, each instance of `android.app.Activity` or its subclasses need to implement the `mil.navy.pan.IPAN` interface. The interface forces the implementing app to override several methods that are related to the data transfer channels that the app uses. A `getPanData(…)` and a `processPanData(…)` are the main methods that force the app to implement a data synchronization scheme. This allows the app developers to focus only on data created and ingested by their own app—all the network setup and teardown is done behind the scenes within the PAN Library. The `IPAN` interface (Code 1. IPAN interface) shows the required methods. The implementing app also needs to instantiate an instance of the `mil.navy.pan.PAN` object and update its life cycle the same as the regular app does. The impact to the implementing app is minimal.

3.2 MANIFEST AND PERMISSIONS

The implementing app also needs to add several items to its app Manifest. First, new permissions to use the PAN-specific hardware is required (Code 2. Permissions). This gives the app permission to use the system hardware that displays when a user is installing the app.

In addition to the permissions, the implementing app must also include an `Intent Filter` (Code 3. Intent filter). The `Intent Filter` registers the app for specific messages from the operating system. The filter includes a mime type string, which needs to be the same as the one returned by `getMimeType()` as defined in the `IPAN` interface.

```
/**
 * Example Activity for integration of PAN library into Activity.
 * Bold items are new to the implementing app.
 */
public class MyApplication extends Activity implements IPAN<MyData extends
Serializable> {
      private final String mimeType =
                     "application/com.example.android.myapplication";
      private PAN<MyData> pan = null;

      @Override public PanData<MyData> getPanData() {
            // create a PanData to send to the client device
            return null;
      }

      @Override public void processPanData(PanData<Note> panData) {
            // synchronize data
      }

      @Override public String getMimeType() {
            return mimeType;
      }

      @Override protected void onCreate(Bundle savedInstanceState) {
            super.onCreate(savedInstanceState);

            pan = new PAN<MyData>(this, this);
            pan.checkNFC();
      }

      @Override public void onNewIntent(Intent intent) {
            super.onNewIntent(intent);
      }

      @Override protected void onResume() {
            super.onResume();
            pan.resumePAN(this, getIntent().getAction());
      }

      @Override protected void onPause() {
            super.onPause();
            this.pan.pausePAN(this.getIntent().getAction());
      }

      @Override protected void onStop() {
            super.onStop();
            this.pan.stopPAN(this.getIntent().getAction());
      }

      @Override protected void onDestroy() {
            super.onDestroy();
            this.pan.destroyPAN(this.getIntent().getAction());
      }
}
```

Code 1. IPAN interface

```xml
<uses-sdk android:minSdkVersion="14" android:targetSdkVersion="16" />


<uses-permission android:name="android.permission.NFC" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
<uses-permission android:name="android.permission.CHANGE_NETWORK_STATE" />
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.BLUETOOTH_ADMIN" />
<uses-permission android:name="android.permission.BLUETOOTH" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-feature android:name="android.hardware.nfc" />
<uses-feature android:name="android.hardware.bluetooth" />
```

Code 2. Permissions.

```xml
<intent-filter android:label="PAN" >
	<action android:name="android.nfc.action.NDEF_DISCOVERED" />
	<category android:name="android.intent.category.DEFAULT" />
	<data android:mimeType="application/com.example.android.myapplication" />
</intent-filter>
```

Code 3. Intent filter.

4. USABILITY

4.1 PAN LIBRARY

The PAN Library is easy to use because the simple built-in user interface, The PAN Library is easy to use. The user is shown a smaller image from the current app along with instructions of "Touch to beam" (see Figure 2. PAN user interface). If the mobile devices are pulled away from each other, the action is automatically canceled. If one user touches the screen to send the NFC message, that mobile device acts at the server, while the other device acts as the client. The server device will then set up the required services to receive a connection from the client.

For some mobile devices, a Bluetooth® connection will then create a popup to make sure the user wants to pair with the second device. This is for increased security, but will only be displayed for the first connection for some manufacturers. Wi-Fi Direct® will always make a user confirm that they want to connect to the second device.

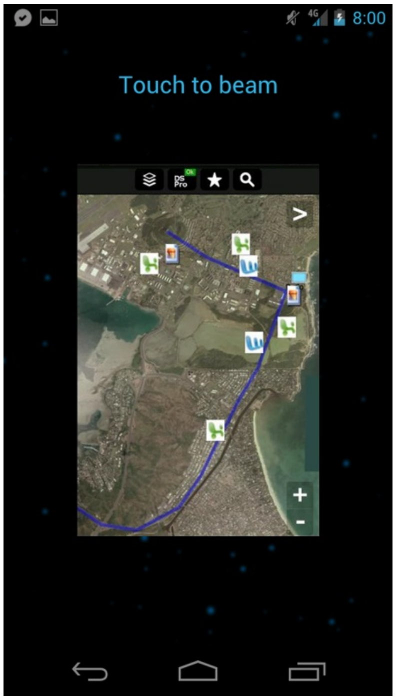

Figure 2. PAN user interface.

4.2 BEST PRACTICES

Although the user interface is simple, it can be unresponsive if the code is incorrect. If the data sent over NFC is large or there is a large amount of computation (see Table 2. PAN data overview), the interface will become unresponsive. This is a result of the built-in NFC capabilities interface and cannot be remedied.

5. RECOMMENDATIONS

5.1 ANDROID VERSIONS

Researchers used Android versions 4.0.4 and 4.1.1 for developing the PAN library. These versions were chosen based on current market availability and external project requirements. Future versions of Android should be backwards compatible with the versions researched, but may add extra capability or stability improvements.

5.1.1 COMPATIBILITY

Testing determined that using the same version on both mobile devices is optimal for best compatibility. When the researchers used two different versions with each other, the networks did not consistently connect. To remedy an unsuccessful connection, the network hardware and the app need a restart.

5.1.2 MIMIMUM VERSIONS

The minimum version recommended for PAN technologies is Version 4.0 (API 14). This minimum gives an acceptable set of application programming interface (API) calls to manage the network technologies. However, a recommended version of 4.1 (API 16) is a better option. API 16 gives more methods to cancel network requests and connection attempts and is more stable.

5.2 SECURITY

Researchers were committed to using built in security procedures and elements. This would ensure industry standards were used for the PAN library. NFC

5.2.1 NFC

NFC does not provide any link encryption. The implementing application must encrypt and decrypt the data sent over NFC. The PAN library has implemented symmetric key 256-bit Advanced Encryption Standard (AES) encryption for data passed over NFC. See `mil.navy.pan.common.Security` for the full encryption implementation.

5.2.2 BLUETOOTH®

The Bluetooth® connection uses the numeric comparison security method as described in Section 5.1.4.1 of the Bluetooth® Specification Version 4.0 published in 2010. This method shows each user a six-digit pin, and asks the two users to confirm they are identical. This ensures that devices were intended for connection, even in situations where multiple devices share the same name. This adds protection against man-in-the-middle attacks. However, the six-digit identification pin is not used for data encryption. Knowing the pin does not add any value for attack.

For key exchange, Bluetooth® uses the Elliptic Curve Diffie-Hellman (ECDH) algorithm. This algorithm thwarts passive eavesdropping (Bluetooth, 2010).

5.2.3 WI-FI DIRECT®

The Wi-Fi Direct® method uses industry standard Wi-Fi Protected Access® 2 (WPA2™). This method includes 256-bit AES encryption with Wi-Fi Protected Setup™ initiation (Wi-Fi Alliance, 2010).

5.3 CODE REUSE

If each tactical mobile app required independent and unique PAN capability, the app would need lots of unnecessary complexity and create duplicate code. The network backend is data agnostic, which means that any type of app could use the PAN Library. Thus, programmers would have to rewrite the library's approximately 2500 lines of code for each app not implementing the library.

6. SUMMARY

Integrating PAN technologies into current and future tactical apps can provide important functionality when units are in adverse environments; the ability to synchronize data without extra equipment is invaluable. The advantages in SWaP is almost reason enough to transition to a tactical handheld solution for command and control at the tactical edge. With the addition of data synchronization at a low cost to development using the PAN Library, it should be a capability integrated into tactical apps.

Based on experimental results, NFC is an ideal technology for bootstrapping a much faster connection. Bluetooth® is highly reliable, but with lower speeds, while Wi-Fi Direct® is much faster, but with lower consistency when connecting devices. Even with the lower reliability, Wi-Fi Direct® has great advantages with large data transfer, both in speed and efficiency.

7. REFERENCES

Standard ECMA-340. 2004 (December). Retrieved from ECMA International: http://www.ecma-international.org/publications/standards/Ecma-340.htm

Standard ECMA-352. 2010 (June). Retrieved from ECMA International: http://www.ecma-international.org/publications/standards/Ecma-352.htm

Bluetooth. (2010). *BLUETOOTH SPECIFICATION Version 4.0.*

Deputy Commandant for Combat Development and Integration. 2013. *FY13 MAGTF C2 Roadmap.* USMC.

Erwin, S. I. 2011 (May). Army, "Marines Face Uphill Battle to Lighten Troops' Tattery Load," *National Defense Magazine*.

ISO/IEC. 2013. "18092:2013 Information Technology -- Telecommunications and Information Exchange between Systems -- Near Field Communication -- Interface and Protocol." ISO/IEC.

Seikkinen, M., M. Hiienkari, J. K. Nurminen, and J. Nieminen. 2012. "How Low Energy is Bluetooth Low Energy? Comparative Measurements with ZigBee/802.15.4." *WCNC Workshop on Internet of Things Enabling Technologies, Embracing Machine-to-Machine Communications and Beyond* (pp. 232–236). Paris, France. IEEE.

Wi-Fi Alliance. 2010. *Wi-Fi CERTIFIED™ Wi-Fi Direct.* Wi-Fi Alliance.

Wi-Fi Alliance. 2013 (June 19). "Wi-Fi CERTIFIED™ ac Takes Wi-Fi Performance to New Heights." Press release. Retrieved 2013, from Wi-fi.org.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-01-0188*

1. REPORT DATE *(DD-MM-YYYY)* August 2014	**2. REPORT TYPE** Final	**3. DATES COVERED** *(From - To)*
4. TITLE AND SUBTITLE Personal Area Networks for Mobile Devices		**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHORS Brian Visser		**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) SSC Pacific, 53560 Hull Street, San Diego, CA 92152–5001		**8. PERFORMING ORGANIZATION REPORT NUMBER** TR 2047
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Science and Technology Initiative SSC Pacific, 53560 Hull Street, San Diego, CA 92152–5001		**10. SPONSOR/MONITOR'S ACRONYM(S)** STI **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release.

13. SUPPLEMENTARY NOTES
This is work of the United States Government and therefore is not copyrighted. This work may be copied and disseminated without restriction.

14. ABSTRACT

The Personal Area Networks (PAN) library was designed to reduce the impact on implementing apps. Therefore, the impact on time and effort is minimal. The app only needs to implement several methods, and manage its own data. Each network type has setup overhead as well as different transmit speeds. For Near Field Communication (NFC), it is recommended to use for data sizes less than 1024 bytes, or to bootstrap another network type. Bluetooth® is recommended for sizes between 1025 bytes and 131072 bytes, and Wi-Fi Direct™ for anything larger. These data size recommendations give the best time and power usage.

15. SUBJECT TERMS
Mission Area: Network Communications

situation awareness	user interface	new field communications
personal area network	Bluetooth®	Wi-Fi Direct®

16. SECURITY CLASSIFICATION OF: a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON / 19B. TELEPHONE NUMBER *(Include area code)*
U	U	U	U	30	Brian Visser (619) 553-3266

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

INITIAL DISTRIBUTION

84300	Library	(2)
85300	Archive/Stock	(1)
53628	B. Visser	(7)

Defense Technical Information Center Fort Belvoir, VA 22060–6218	(1)

Approved for public release.

SSC Pacific
San Diego, CA 92152-5001